- Do not ask clients for testimonials or reviews;
- Make "Googling" your clients an informed consent issue.

Training in the Uses of Technology in Counselling and Psychotherapy

Training in the uses of technology in counselling and psychotherapy is available through a number of reputable programs in Canada, the UK and the USA. If you are considering pursuing additional training in this area you may want to consider some of the following when choosing your course.

Who is teaching the course and what is their experience in this field? Do they participate in research as well?

Does the course address: ethical, technological and practical considerations such as goodness of fit for client and modality, backup communication and crisis planning?

Does the course address the differences between face-to-face and online therapeutic relationships?

Glossary of Terms

Apps
An abbreviation for "application." It's a piece of software that can run through a web browser or even offline on your computer, phone, tablet or any other electronic device. Apps may or may not have a connection to the Internet.

Asynchronous Text-Based Counselling
In this modality of counselling the mode of communication is text and the client and counsellor or psychotherapist do not have to be sitting at their computer at the same time, resulting in a stretched timeframe in which interaction occurs.

Augmented Reality
A live direct or indirect view of a physical, real-world environment whose elements are "augmented" by computer-generated or real world extracted sensory input. Augmented reality enhances one's current perception of reality.

Avatar
An electronic image that represents and is manipulated by a computer user in a virtual space (as in a computer game or an online shopping site) and that interacts with other objects in the space.

Backup Systems
The process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost.

Backup Policy
A pre-defined, set schedule whereby information from business applications such as Oracle, Microsoft SQL, email server databases and user files is copied to disk and/or tape to ensure data recoverability in the event of accidental data deletion, corrupted information or some kind of a system outage. It can also be an organisation's procedures and rules for ensuring that adequate amounts and types of backups are made, including suitably frequent testing of the process for restoring the original production system from the backup copies.

Big Data
'Big data' is the new science of understanding and predicting human behaviour by studying large volumes of unstructured data. Big data is also known as 'predictive analytics'. For example, analyzing Twitter posts, Facebook feeds, eBay searches, GPS trackers, and ATM machines.

Bitcoin
A type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

The Cloud
Cloud storage is a term that refers to online space that you can use to store your data. The simplest type of cloud storage occurs when users upload files and folders on their computers or mobile devices to an Internet server. The uploaded files serve as a backup in case the original files are damaged or lost. Using a cloud server permits the user to download files to other devices when needed. The files are typically protected by encryption and are accessed by the user with login credentials and password. The files are always available to the user, as long as the user has an Internet connection to view or retrieve them.

Cryptocurrency
Cryptocurrency is a type of digital currency that uses cryptography for security and anti-counterfeiting measures. Public and private keys are often used to transfer cryptocurrency between individuals.

Data Removal App
An app that allows you to securely remove data and documents from any of your devices. This can be done in-person or remotely in case the device is lost or stolen.

Digital Divide
Refers to the gap between demographics and regions that have access to modern information and communications technology and those that don't or have restricted access. This can include telephone, television, computers and the Internet.

Disinhibition
People may behave differently online/when using other media to the ways in which they might interact in face-to-face situations. They may disclose information more quickly than they would in face-to-face situations. They may also be uninhibited in their expressions of emotions (e.g. more insensitive or angry). These differences in behaviour may be influenced by the following features of the online environment:

- Having the sense of being anonymous and invisible
- Not seeing (and therefore not experiencing) other people's reactions to what is said' experiencing an absence of external authority in the online/other media environment
- Not experiencing others as 'real'

Encryption
Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.

Firewalls
A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet.

Hardware
The physical parts or components of a computer, such as the monitor, keyboard, computer data storage, graphic card, sound card and motherboard. Hardware is directed by the software to execute any command or instruction.

Malware
Malware, a shortened combination of the words **mal**icious and soft**ware**, is a catch-all term for any sort of software designed with malicious intent. That *malicious intent* is often theft of your private information or the creation of a backdoor to your computer so someone can gain access to it without your permission. However, software that does *anything* that it didn't tell you it was going to do could be considered malware.

Password Protection
A security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

Personal Information
Any information about an identifiable individual but does not include business contact information (e.g. individual's title, business telephone number, business address, business email or facsimile number).

Personal Health Information
Recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual.

Phishing
A fraudulent practice in which private data is captured on websites or through an email designed to look like a trusted third party. Typically, phishing (from "password fishing") scams involve an email alerting the user to a problem with their bank or another account.

Presence Techniques
The text-based therapeutic techniques that allow psychotherapists and counsellors to overcome the absence of tone of voice and non-verbals in asynchronous text-based counselling.

Privacy Impact Assessment (PIA)
An analysis of how an individual's or groups of individuals' personally identifiable information is collected, used, shared and maintained by an organization. A process used to evaluate and manage privacy impacts and to ensure compliance with privacy protection rules and responsibilities. You can find templates for PIAs on provincial and federal privacy websites.

Ransomware
Ransomware is a form of malware that encrypts files on an infected device and holds them hostage until the user pays a ransom to the malware operators.

Real Time Chat
A real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly.

Software
The part of the computer system that consists of data or computer instructions

Spear Phishing
A Spear Phishing email is similar to a Phishing email, but it is specifically targeted to either an individual or an organization. For example, an email might go out to everyone at a university telling them to click a link where you are asked to provide your login information.

Spoofed
A spoofed Wi-Fi will give you Internet access while stealing the login information for any site you visit.

Synchronous Communications
Interactions between client and counsellor or psychotherapist at the same point in time.

Text-Based Counselling
The use of 'text only' as the modality for counselling.

Text Messaging
The act of composing and sending electronic messages, typically consisting of alphabetic and numeric characters, between two or more users of mobile phones, tablets, desktops/laptops, or other devices. Text messages may be sent over a cellular network or may also be sent via an Internet connection.

Therapist-Assisted Online Mental Health Treatment Programs
Model of mental health service delivery that combines the use of web-based interactive resources with brief weekly online sessions with a counsellor.

Third-Party Services
A third party is an entity that is involved in some way in an interaction that is primarily between two other entities. The third party may or may not be officially a part of the transaction between the two primary entities and may or may not be interacting transparently and/or legally.

2-Factor Authentication
2-Factor Authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.

Video Counselling
A synchronous counselling service where the client and counsellor or psychotherapist communicate using a webcam, land line, and encrypted Internet software through which both parties are able to see and hear each other and are able to share and create documents in real-time.

Virtual Private Network
A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods — including passwords, tokens and other unique identification methods — to gain access to the VPN.

Virtual Reality
The computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors.

Wearable Technologies
A category of technology devices that can be worn by a consumer and often include tracking information related to health and fitness.

APPENDIX A – Detailed Data Protection Measures

Phishing and Spear Phishing Tips

These tips will help you mitigate the threat:

- If you receive an email that has an attachment in it and there is a request for you to open the attachment, look to see if the email address is actually from the person it says it is from. Click on the name and look at the email address;
- If you are at all suspicious do not open or download the file. Contact the person and ask them if they sent you something;
- Banks don't send attachments. Businesses don't send invoices out of the blue. Always take a moment and think about what you are looking at. Did you recently order something from this business?
- Links in Phishing emails will often look like they are from yourbank.com/login. But the link will take you to another website. Always check the URL of the site you are on after you follow the link. If, for example, it says: http://www.thieves.com/rbc/login it is not the Royal Bank of Canada;
- If you are unsure whether an email is safe or not assume it is unsafe. Do not click on the link. Contact the institution and ask them if they are sending out emails;
- Companies in Canada and around the globe know about phishing. They do not send out emails asking you to provide your login information. Your company, agency or institution will not send you an email asking for your login and password information. If you receive an email like this you should not trust it.

Stingrays and IMSI Catchers[29]

Progress in technology is much like an arms race. The bad guys develop a new virus, the good guys develop a new way or catching and defeating that virus. A new security hole is discovered that the bad guys can use to steal your personal information. The good guys plug that hole.

A recent advancement in the race to steal information is what is known as a Stingray. Every cell phone has an identity number (the IMSI) that it sends to a cell tower in order to communicate through that tower. Devices called Stingrays can mimic the behavior of the tower and catch those numbers. They can then track the device. The more sophisticated Stingrays copy all the information sent from the phone.

Reconsider your plan to use smartphone texting to connect with clients. A better solution is to use an app or service that ensures encryption of data. Be aware of your surroundings and take care in any situation in which sensitive information is being communicated over a mobile system.

[29] See, for example, https://privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions

Wi-Fi Tips

- If you use Wi-Fi at your place of business ensure it is secured;
- Do not use public Wi-Fi for sensitive information because public wireless services are not secure even when password protected;
- Consider using your own cell data in public places;
- Use a Virtual Private Network (VPN) (which is designed to provides a secure, encrypted tunnel in which to transmit data);
- Watch for 'spoofed' Wi-Fi. For example, you might be in Starbucks and there are 3 Wi-Fi networks: Starbucks, Starbucks Toronto, and Starbucks Local. Inform the manager of this and find out which is the real one. A spoofed Wi-Fi will give you Internet access while stealing the login information for any site you visit;
- Make sure your home Wi-Fi is secure;
- If you have Wi-Fi do not allow guests onto your Wi-Fi. You risk the spread of viruses;
- If you have multiple computers on your Wi-Fi network, and you enable file sharing on those computers, letting someone onto your network potentially exposes the data in those folders. It is easy to setup a separate Wi-Fi network for guests.

APPENDIX B – Checklist for the Uses of Technology in Clinical Supervision

Modalities for clinical supervision include but are not limited to:

- Telephone (landline, cell or smartphone)
- Digital/video recording that is shared with supervisor
- Videoconferencing
- Text or chat messaging
- Email
- Live supervision via videoconference of face-to-face session or virtual reality session

Choose the technology that best meets the needs of your supervisees and consider:

- Availability
- Affordability
- Reliability
- Privacy
- Security
- How the technology may affect the working alliance

Informed consent for both the supervisee and the client needs to include:

- How information will be kept confidential
- How to communicate in case of a technical failure
- Limitations of technology/modality
- Potential risks of technology/modality
- Potential benefits of technology/modality
- Emergency plan for client crisis
- Social media policy

What to discuss with your supervisee:

- Sign and adhere to a clinical supervision contract
- Challenges of using technology and how it may impact communication
    - For example, silences when using telephone or video. What do you both consider to be an acceptable length of time to be in silence before initiating conversation?
- Minimizing distractions and avoiding unrelated multi-tasking during supervision time
- When is it important to use face-to-face or phone to discuss sensitive information?
- Social media policy
- Responsibility for maintaining privacy and security rests with both the supervisor and the supervisee
- May need to factor in additional time for supervision

Supervisors' knowledge, skills for using technology in clinical supervision:

- Capacity to use the technology with basic skills and an ability to trouble shoot
- Supervisor needs to keep current on the types of technology and potential uses
- Need to demonstrate and promote good practice by the supervisee to protect client privacy and confidentiality
- Supervisor must know how to minimize risk associated with transferring and storing sensitive data
- Need to screen supervisee's appropriateness to receive supervision via distance methods and ensure supervisee's screen clients
- Provide readings and guidelines on professionalism, privacy/security and ethics regarding technology
- Must be able to demonstrate an ability to translate best practices in clinical supervision to the technology-based format
- Must be able to articulate the reasons for the choice of technology platform
- Prepare and practice using the technology and get comfortable with the technology's privacy settings
- Understanding of the potential disinhibition effects on supervisees and yourself
- Stay up to date on legislation and the professional ethics of the supervisee's association
- Develop an understanding of the implications of technology for you as a supervisor
- Become informed about vicarious liability

If you are seeking supervision, you should only consult with someone who has experience and training in working online. It can be helpful to be supervised in the same modality in which you are working.

<u>Good practice tips for the uses of various technologies in clinical supervision:</u>
For all modalities, never discuss personal health information unless the technology is secure, password protected and has been vetted by you for compliance with the relevant privacy laws.

Telephone (landline, cellular or smartphone)

- Conduct calls only in private, closed office
- Use a head set to improve sound quality
- Avoid using public or unsecured Wi-Fi for calls on a mobile phone

Video Conferencing

- Have a back-up communication plan in case of technical failure
- Ensure privacy
- Limit distractions

Digital Video or Audio Recording

- Ensure security protocols are in place for recording, transmitting, archiving and destroying the recording
- Camera on counsellor only

Email

- Encrypt all emails
- Pay attention to tone and learn ways to compensate for lack of visual cues

File Sharing

- Thoroughly vet any cloud-based storage for compliance with privacy laws
- Ensure sending and receiving devices are compliant as well
- Use encryption software to share files
- Use passwords and highest privacy settings
- Screen sharing can be useful

Text/Chat Messaging

- Clarify with supervisee when it would be appropriate to use text or chat
- Use only for simple, non-confidential conversations
- Practice using this modality for clarity and brevity